Agency 7
Secretary of State

Articles

Article 16.—FEES

7-16-1. Information and services fee. In addition to any other fees specified in regulation or statute, the fees prescribed in the secretary of state's "schedule of information and services fees," dated May 27, 2010 and hereby adopted by reference, shall be charged by the secretary of state. (Authorized by and implementing K.S.A. 2009 Supp. 75-438 and L. 2009, ch. 47, sec. 35; effective, T-7-7-1-03, July 1, 2003; effective Oct. 10, 2003; amended Oct. 31, 2008; amended, T-7-7-1-10, July 1, 2010; amended Sept. 10, 2010.)

Article 41.—KANSAS UNIFORM ELECTRONIC TRANSACTIONS ACT

7-41-1. Definitions. (a) "Certificate" means a computer-based record or electronic message that at a minimum meets the following conditions:

(1) Identifies the registered certification authority issuing the certificate;

(2) names or identifies a subscriber;

(3) contains the public key of the subscriber;

(4) identifies the period of time during which the certificate is effective; and

(5) is digitally signed by the registered certification authority.

(b) "Certificate policy" means the policy that identifies the applicability of a certificate to particular communities and classes of applications with common security requirements. This term is also known as "CP."

(c) "Certificate revocation list" means a list maintained by a registered certification authority of the certificates the registered certification authority has issued that are revoked before their stated expiration dates. This term is also known as "CRL."

(d) "Certification practice statement" means a statement published by a registered certification authority that specifies the policies or practices that the registered certification authority employs in issuing, publishing, suspending, revoking, and renewing certificates. This term is also known as "CPS."

(e) "Compliance review" means documentation in the form of an information systems audit report verifying that the applicant or registered certification authority has the use of a trustworthy system as defined in subsection (r).

(f) "Identification and authentication" means the process of ascertaining and confirming through appropriate inquiry and investigation the identity of a certificate applicant in compliance with the requirements for certificate security levels specified in the ITEC certificate policy or the CP. This term is also known as "I and A."

(g) "Information technology executive council" means the Kansas information technology executive council, pursuant to K.S.A. 75-7201 et seq. and amendments thereto, and is also known as "ITEC."

(h) "Information technology executive council policy 9200" means the "certificate policy for the state of Kansas public key infrastructure," version 2, including the appendices, approved by the ITEC, amended on April 24, 2008, and hereby adopted by reference. This document applies to state agencies offering or providing the option of using a digital signature to persons with whom the state agencies do business. This term is also known as "ITEC certificate policy."

(i) "Information technology identity management group" means the group that has been delegated authority by the ITEC and is authorized by the ITEC to make day-to-day administrative and fiscal decisions for the public key infrastructure program. This term is also known as "ITIMG."

(j) "Local registration authority" means a person operating under the ITEC certificate policy that has a relationship of trust with a community of potential subscribers and, for that reason, has

a contractual relationship with a registration authority to perform duties including accepting applications and conducting identification and authentication for certificate applicants in accordance with the law, the ITEC certificate policy, and the appended agreements. This term is also known as "LRA."

(k) "Local registration authority's trusted partner" means a person operating under the ITEC certificate policy that has a relationship of trust with an LRA and that executes a trusted partner agreement with an LRA, as contained in the appendices to the ITEC certificate policy, in order to secure LRA services for the community of potential subscribers of the local registration authority's trusted partner. This term is also known as "LRA's trusted partner."

(l) "Private key" means the key in a subscriber's key pair that is kept secret and is used to create digital signatures and to decrypt messages or files that were encrypted with the subscriber's corresponding public key.

(m) "Public key" means the key in a subscriber's key pair that can be used by another person to verify digital signatures created by a subscriber's corresponding private key or to encrypt messages or files that the person sends to the subscriber.

(n) "Public key infrastructure" means the architecture, organization, techniques, practices, policy, and procedures that collectively support the implementation and operation of a certificate-based, public key cryptography system. This term is also known as "PKI."

(o) "Registered certification authority" has the meaning specified in K.S.A. 16-1602, and amendments thereto. This term is also known as "registered CA."

(p) "Registration authority" means a person operating under the ITEC certificate policy who has been authenticated by a registered CA, issued a registration authority certificate by the registered CA, approved by the ITEC to process subscriber applications for certificates and, if required by the ITEC certificate policy, to conduct I and A of certificate applicants in accordance with the law, the ITEC certificate policy, and the appended agreements. This term is also known as "RA."

(q) "Subscriber" means a person operating under the ITEC certificate policy who meets the following criteria:

(1) Is the subject of a certificate;

(2) accepts the certificate from a registered certification authority; and

(3) holds the private key that corresponds to the public key listed in that certificate.

(r) "Trustworthy system" means a secure computer system that materially satisfies the most recent common criteria protection profile for commercial security, known as "CSPP — guidance for COTS security protection profiles," published by the U.S. department of commerce in December 1999 and hereby adopted by reference.

(s) "X.509" means the standard published by the international telecommunication union-T (ITU-T) in March 2000 that establishes a model for certificates. This X.509 standard, including annexes A and B, is hereby adopted by reference. (Authorized by K.S.A. 16-1605 and 16-1618; implementing K.S.A. 16-1605, 16-1617, and 16-1619; effective July 6, 2001; amended Aug. 19, 2005; amended March 6, 2009.)

7-41-2. Original registration; renewal; expiration. (a) Each original registration or renewal registration for a registered certification authority shall expire one year from the date of issuance.

(b) Each renewal application for registration shall be deemed timely if the registered certification authority files a renewal application with the secretary of state within 60 days before the date the original application or renewal application otherwise will expire. (Authorized by K.S.A 16-1618; implementing K.S.A. 16-1617; effective July 6, 2001; amended March 6, 2009.)

7-41-3. Registration forms. (a) Each person, before performing the duties of a registered certification authority, shall register with the secretary of state on forms prescribed by the secretary of state.

(b) Original applications, renewal applications, and other information may be allowed by the secretary of state to be filed electronically.

(c) Each applicant for registered certification authority shall file the following with the original application or renewal application:

(1) A compliance review with a report date within 90 days of the original application or renewal application date;

(2) a copy of the applicant's certification practice statement and CP;

(3) a nonrefundable original application or renewal application fee of $1,000; and

(4) a good and sufficient surety bond, certificate

of insurance, or other evidence of financial security in the amount of $100,000. (Authorized by K.S.A. 16-1618; implementing K.S.A. 16-1617; effective July 6, 2001; amended March 6, 2009.)

7-41-4. Evidence of financial security. The evidence of financial security shall include, in addition to the requirements of K.S.A. 16-1617 and amendments thereto, the following: (a) The identity of the insurer or the financial institution issuing the surety bond, certificate of insurance, or irrevocable letter of credit, including the following information:

(1) The name;

(2) the mailing address;

(3) the physical address; and

(4) the identification, by number or copy of appropriate documentation, of the licensure or approval as a financial institution or as an insurer in this state;

(b) the identity of the registered certification authority on behalf of which the evidence of financial security is issued;

(c) a statement that the evidence of financial security is issued payable to the secretary of state for the benefit of persons holding qualified rights of payment against the registered certification authority named as principal of the surety bond, certificate of insurance, or irrevocable letter of credit;

(d) a statement that the evidence of financial security is issued for filing pursuant to the Kansas uniform electronic transactions act and amendments thereto; and

(e) a statement of term that extends at least as long as the term of the registration to be issued to the registered certification authority. (Authorized by K.S.A. 16-1618; implementing K.S.A. 16-1617; effective July 6, 2001; amended March 6, 2009.)

7-41-5. Certification practice statement. Each registered certification authority shall file with the secretary of state a certification practice statement as required by K.A.R. 7-41-3. The statement shall declare the practices that the registered certification authority uses in issuing, suspending, revoking, and renewing certificates. The statement shall also include the following information: (a) If certificates are issued by security levels, the necessary criteria for each certificate security level, including the methods of certificate applicant identification applicable to each security level;

(b) disclosure of any warnings, liability limitations, warranty disclaimers, and indemnity and hold harmless provisions, if any, upon which the registered certification authority intends to rely;

(c) disclosure of any and all disclaimers and limitations on obligations, losses, or damages, if any, to be asserted by the registered certification authority;

(d) a written description of all representations from the certificate applicant required by the registered certification authority relating to the certificate applicant's responsibility to protect the private key; and

(e) disclosure of any mandatory dispute resolution process, if any, including any choice of forum and choice of law provisions. (Authorized by K.S.A. 16-1618; implementing K.S.A. 16-1617; effective July 6, 2001; amended March 6, 2009.)

7-41-6. Changes to information. Each original applicant or renewal applicant for a registered certification authority shall notify the secretary of state about any change to its CP, CPS, or information contained in its original application or renewal application, as the CP, CPS, or information appears in the secretary of state's files, within 30 days of the effective date of the change. (Authorized by K.S.A. 16-1618; implementing K.S.A. 16-1617; effective July 6, 2001; amended March 6, 2009.)

7-41-7. Recordkeeping and retention of registered certification authority documents. Each registered certification authority shall maintain documentation of compliance with the Kansas uniform electronic transactions act and this article. The documentation shall include evidence demonstrating that the registered certification authority has met the following requirements:

(a) Each registered certification authority shall retain its records of the issuance, acceptance, and any suspension or revocation of a certificate for a period of at least 10 years after the certificate is revoked or expires. The registered certification authority shall retain custody of the records unless it ceases to act as a registered certification authority.

(b) All records subject to this article shall be in the English language. (Authorized by K.S.A. 16-1618; implementing K.S.A. 16-1617; effective July 6, 2001; amended March 6, 2009.)

7-41-8 and 7-41-9. (Authorized by K.S.A. 2000 Supp. 16-1618; implementing K.S.A. 2000

Supp. 16-1617; effective July 6, 2001; revoked March 6, 2009.)

7-41-10. Procedure upon discontinuance of registered certification authority business. Each registered certification authority that discontinues providing registered certification authority services without making other arrangements for the preservation of the registered certification authority's records shall notify the secretary of state and the subscribers, in writing, of its discontinuance of business. (Authorized by K.S.A. 16-1618; implementing K.S.A. 16-1617; effective July 6, 2001; amended March 6, 2009.)

7-41-11. Recovery against financial security. (a) In order to recover against a registered certification authority's surety bond, certificate of insurance, or other evidence of financial security, the claimant shall meet the following requirements:

(1) File a signed notice of the claim with the secretary of state, providing the following information:

(A) The name and address of the claimant;

(B) the amount claimed;

(C) the grounds for the qualified right to payment; and

(D) the date of the occurrence forming the basis of the claim; and

(2) attach to the notice a certified copy of the judgment upon which the qualified right to payment is based, except as provided in subsection (b).

(b) If the notice specified in this regulation is filed before entry of judgment, the notice shall be held on file by the secretary of state, without further action, until the claimant files a copy of the judgment. If the secretary of state determines that the action identified in the notice finally has been resolved without a judgment awarding the claimant a qualified right to payment, the notice may be expunged by the secretary of state from the secretary of state's records. A notice shall not be expunged by the secretary of state until two years have elapsed since the notice first was filed.

(c) A notice for filing shall be rejected by the secretary of state if the date of the occurrence forming the basis for the complaint is more than two years before the filing of the notice.

(d) If the notice and judgment are filed pursuant to paragraphs (a)(1) and (2), a copy of the notice and judgment shall be provided by the secretary of state to the surety, insurer, or issuer of the financial security for qualified right of payment to the claimant. (Authorized by K.S.A. 16-1618; implementing K.S.A. 16-1617; effective July 6, 2001; amended March 6, 2009.)

7-41-12. Reciprocity. (a) Any registered certification authority that is licensed, registered, or otherwise under the statutory oversight of a governmental agency, as defined by the Kansas uniform electronic transactions act and amendments thereto, may be registered as a registered certification authority in Kansas if all of the following conditions are met:

(1) The oversight of the governmental agency is equal to or greater than the oversight required pursuant to the Kansas uniform electronic transactions act and amendments thereto and this article.

(2) The registered certification authority submits to the secretary of state a written request for registration and a copy of the license or registration issued by the governmental agency.

(3) The registered certification authority pays the $1,000 application fee.

(b) Each registered certification authority registered pursuant to this regulation shall be exempt from the provisions of K.A.R. 7-41-3(c)(1).

(c) If the information filed pursuant to this regulation is satisfactory to the secretary of state, a registered certification authority may be issued a Kansas reciprocal registration by the secretary of state. (Authorized by K.S.A. 16-1618; implementing K.S.A. 16-1619; effective July 6, 2001; amended March 6, 2009.)

7-41-13. Use of subscriber information. Each registered certification authority shall use subscriber and certificate applicant information only for the purpose of performing the identification and authentication process. (Authorized by K.S.A. 16-1618; implementing K.S.A. 16-1617; effective July 6, 2001; amended March 6, 2009.)

7-41-14. State agency; compliance. Each state agency offering or providing the option of using a digital signature to persons doing business with the state agency shall meet either of the following requirements:

(a)(1) Become an LRA by executing an agreement with the RA, as contained in the appendices to the ITEC certificate policy; and

(2) perform the duties of an LRA in accordance with the ITEC policy and these regulations; or

(b)(1) Become an LRA's trusted partner by executing a trusted partner agreement with an LRA,

as contained in the appendices to the ITEC certificate policy; and

(2) perform the duties of an LRA's trusted partner in accordance with the ITEC certificate policy and these regulations. (Authorized by and implementing K.S.A. 16-1605; effective Aug. 19, 2005; amended March 6, 2009.)

7-41-15. Registration authority, local registration authority, and local registration authority's trusted partner; compliance. Each RA, LRA, and LRA's trusted partner shall meet the following requirements:

(a) Comply with these regulations and the ITEC certificate policy when administering any certificate or the associated keys; and

(b) ensure that I and A procedures are implemented in compliance with the requirements for certificate security levels specified in the ITEC certificate policy. (Authorized by and implementing K.S.A. 16-1605; effective Aug. 19, 2005; amended March 6, 2009.)

7-41-16. Registration authority, local registration authority, and local registration authority's trusted partner; general responsibilities. (a) Each RA, LRA, and LRA's trusted partner shall perform that party's duties in a manner that meets the following requirements:

(1) Complies with the ITEC certificate policy;

(2) promotes a cooperative relationship with registered CAs; and

(3) uses keys and certificates issued by a registered CA only for authorized purposes.

(b) The primary duties of each RA, LRA, or LRA's trusted partner shall be the following:

(1) The establishment of a trustworthy environment and procedure for certificate applicants to submit applications;

(2) the I and A of each person applying for a certificate or requesting a certificate renewal or a certificate update in compliance with the requirements for certificate security levels specified in the ITEC certificate policy;

(3) the approval or rejection of certificate applications; and

(4) the revocation of certificates at the request of the subscriber or other authorized persons or upon the initiative of the RA, LRA, or LRA's trusted partner. (Authorized by and implementing K.S.A. 16-1605; effective Aug. 19, 2005; amended March 6, 2009.)

7-41-17. Registration authority, local registration authority, and local registration authority's trusted partner; certification. Each RA, LRA, and LRA's trusted partner shall certify on a form prescribed by the ITIMG that the RA, LRA, or LRA's trusted partner has secured an individual subscriber application from a certificate applicant and authenticated the certificate applicant's identity in compliance with the requirements for certificate security levels specified in the ITEC certificate policy when submitting certificate applicant information to an LRA, the RA, or a registered CA. (Authorized by and implementing K.S.A. 16-1605; effective Aug. 19, 2005; amended March 6, 2009.)

7-41-18 through 7-41-29. (Authorized by and implementing K.S.A. 2004 Supp. 16-1605; effective Aug. 19, 2005; revoked March 6, 2009.)

7-41-30. Identification and authentication; certificate security levels. Each RA, LRA, and LRA's trusted partner shall ensure that the applicable requirements for certificate security levels specified in the ITEC certificate policy are met when conducting the I and A of a certificate applicant. (Authorized by and implementing K.S.A. 16-1605; effective Aug. 19, 2005; amended March 6, 2009.)

7-41-31. (Authorized by and implementing K.S.A. 2004 Supp. 16-1605; effective Aug. 19, 2005; revoked March 6, 2009.)

7-41-32. Agreements; registration authority; local registration authority; local registration authority's trusted partner; certificate applicant. Each RA, LRA, LRA's trusted partner, and certificate applicant shall execute the agreements contained in the appendices of the ITEC certificate policy when contracting for certificate services. The agreements shall be executed before the issuance, administration, or use of the certificates. (Authorized by and implementing K.S.A. 16-1605; effective Aug. 19, 2005; amended March 6, 2009.)

7-41-33. Picture identification credentials. Each facial image identification required by an RA, LRA, or LRA's trusted partner for the purpose of I and A shall meet the minimum acceptable standards used in the identification credentials specified in the ITEC certificate policy for certificate security levels. (Authorized by and im-

plementing K.S.A. 16-1605; effective Aug. 19, 2005; amended March 6, 2009.)

7-41-34. Certificate; format and name. Each certificate issued by a registered CA for use by a state agency pursuant to K.S.A. 16-1605, and amendments thereto, shall be in the X.509 format and contain a distinguished name in compliance with the ITEC certificate policy. (Authorized by and implementing K.S.A. 16-1605; effective March 6, 2009.)

7-41-35. Registered certification authority; ITEC certificate policy. Each person who performs the duties of a registered certification authority and issues certificates used by a state agency pursuant to K.S.A. 16-1605, and amendments thereto, shall comply with the ITEC certificate policy. (Authorized by K.S.A. 16-1605 and 16-1618; implementing K.S.A. 16-1605 and 16-1617; effective March 6, 2009.)